PATENT ABSTRACTS OF JAPAN

(11)Publication number : 06-006347
(43)Date of publication of application : 14.01.1994

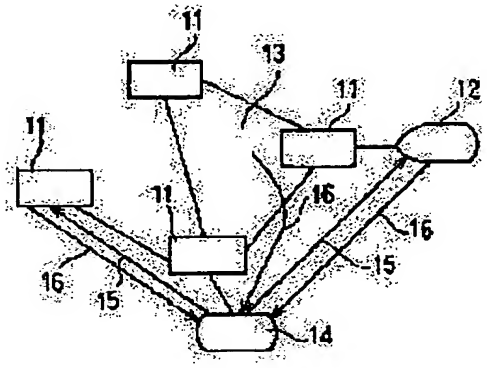
(51)Int.Cl. H04L 9/00
H04L 9/10
H04L 9/12
H04L 12/28

(21)Application number : 04-164743
(22)Date of filing : 23.06.1992

(71)Applicant : MITSUBISHI ELECTRIC CORP
(72)Inventor : AONO HIDEKI

(54) SECURITY MANAGEMENT SYSTEM

(57)Abstract:
PURPOSE: To unify the security level and to relieve the load of management by devising centralized security management.
CONSTITUTION: A management equipment 14 sets security information 15 to a network component equipment 11 and a data processing unit 12 being components of the network system as managed equipments respectively and receives an illegal access report 16 representing a fact of an illegal access from the network c mponent equipment 11 and the data processing unit 12 to manage centralizingly the security of the equipments 11, 12 or the like.



LEGAL STATUS

[Date of request for examination] 18.07.1996
[Date of sending the examiner's decision of rejection] 12.09.2000
[Kind of final disposal of application other than the xaminer's decision of rejection or application converted r gistration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rej ction]
[Date of extinction f right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平６－６３４７

(43)公開日　平成６年（１９９４）１月１４日

(51)Int.Cl.[5]	識別記号	庁内整理番号	Ｆ Ｉ	技術表示箇所
H04L 9/00				
9/10				
9/12				
12/28				
		7117-5K	H04L 9/00	Z

審査請求　未請求　請求項の数１　（全５頁）　最終頁に続く

(21)出願番号　特願平４－１６４７４３

(22)出願日　平成４年（１９９２）６月２３日

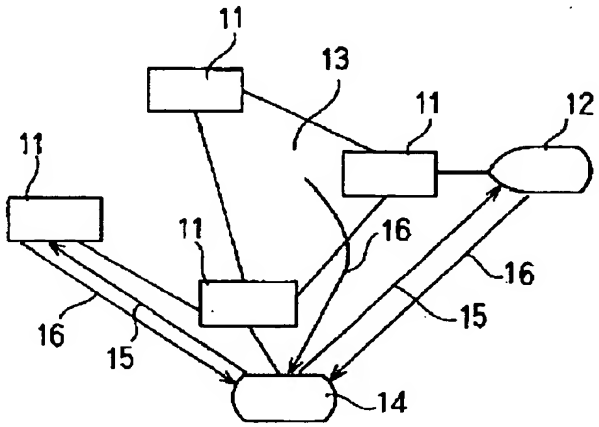
(71)出願人　０００００６０１３
三菱電機株式会社
東京都千代田区丸の内二丁目２番３号

(72)発明者　青野　英樹
鎌倉市上町屋３２５番地　三菱電機株式会社コンピュータ製作所内

(74)代理人　弁理士　曾我　道照　（外６名）

(54)【発明の名称】セキュリティ管理システム

(57)【要約】
【目的】　集中的にセキュリティ管理ができるようにし、セキュリティレベルを統一できると共に、管理の手間を軽減できるセキュリティ管理システムを提供する。
【構成】　１３は複数のネットワーク構成機器１１で構成したネットワークである。１２はネットワーク１３に接続したコンピュータ等のデータ処理装置である。１４は集中セキュリティ管理装置である。管理装置１４は、被管理装置としてのネットワークシステムを構成するネットワーク構成機器１１、データ処理装置１２に対して夫々セキュリティ情報１５を設定すると共に、ネットワーク構成機器１１、データ処理装置１２より不正アクセスがあったことを示す不正アクセス報告１６を受け取り、機器等１１，１２のセキュリティを集中して管理する。



11：ネットワーク構成機器
12：データ処理装置
13：ネットワーク
14：集中セキュリティ管理装置
15：セキュリティ情報
16：不正アクセス報告

1

【特許請求の範囲】

【請求項１】　被管理装置を構成する複数の機器のセキュリティを集中して管理するセキュリティ管理装置を備え、

上記セキュリティ管理装置は、上記複数のの機器にそれぞれセキュリティ情報を設定すると共に、上記複数の機器より不正アクセスがあったことを示す不正アクセス報告を受け取ることを特徴とするセキュリティ管理システム。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】この発明は、セキュリティ管理を必要とする例えばネットワークにおいて不正アクセスを防ぐのに使用して好適なセキュリティ管理システムに関する。

【０００２】

【従来の技術】図４は、或るネットワークにおける従来のセキュリティ管理システムを示す構成図である。図において、１３は複数のネットワーク構成機器１１として例えば多重化装置で構成されるネットワークである。

【０００３】ネットワーク１３には、コンピュータ等のデータ処理装置１２が接続される。これらネットワーク構成機器１１、データ処理装置１２に対する不正アクセス４１のセキュリティ管理は、各機器等１１，１２が独立して行っている（管理装置またはコンソールは図示せず）。

【０００４】次に動作について説明する。図５は従来のセキュリティ管理システムの動作を示すフローチャートである。まず、各システム、機器の管理装置またはコンソールよりセキュリティ情報をネットワーク構成機器１１、データ処理装置１２に設定する（ステップ５１）。ネットワーク構成機器１１、データ処理装置１２は、それぞれ独自に不正アクセス発見メカニズムを持ち、それに従って不正アクセス４１を発見する（ステップ５２）。そして、各機器等１１，１２は、それぞれの報告規則（例えばログ出力、管理者へのアラーム発生、コンソール表示等）に従って不正アクセスがあったことを報告する（ステップ５３）。

【０００５】

【発明が解決しようとする課題】従来のセキュリティ管理システムは以上のように構成されているので、ネットワーク１３内のセキュリティの管理は、各機器等１１，１２の管理者、使用者単位に行わなければならず、セキュリティレベルを統一できない、管理に手間がかかる、集中的にセキュリティ管理ができない等の問題点があった。

【０００６】この発明はこのような問題点を解決するためになされたもので、集中的にセキュリティ管理ができるようにし、セキュリティレベルを統一できると共に、管理の手間を軽減できるセキュリティ管理システムを提

2

供することを目的とする。

【０００７】

【課題を解決するための手段】この発明に係るセキュリティ管理システムは、被管理装置を構成する複数の機器のセキュリティを集中して管理するセキュリティ管理装置を備え、セキュリティ管理装置は、複数の機器にそれぞれセキュリティ情報を設定すると共に、これら複数の機器より不正アクセスがあったことを示す不正アクセス報告を受け取るものである。

【０００８】

【作用】この発明においては、セキュリティ管理装置によって被管理装置としての複数の機器にそれぞれセキュリティ情報が設定されると共に、このセキュリティ管理装置は複数の機器より不正アクセスがあったことを示す不正アクセス報告を受け取るため、セキュリティ管理装置によって複数の機器を集中して管理することが可能となる。これにより、被管理装置としての複数の機器のセキュリティレベルが統一され、また管理の手間が軽減されることになる。

【０００９】

【実施例】実施例１．図１はこの発明に係るセキュリティ管理システムの一実施例を示す構成図である。図１において、図４と対応する部分には同一符号を付し、その詳細説明は省略する。

【００１０】本例において、１４は集中セキュリティ管理装置である。集中セキュリティ管理装置１４は、被管理装置としてのネットワークシステムを構成するネットワーク構成機器１１、データ処理装置１２に対してそれぞれセキュリティ情報設定要求を送信してセキュリティ情報１５を設定できるように構成する。また本例において、ネットワーク構成機器１１、データ処理装置１２に上述設定されたセキュリティ情報１５に対してそれを犯す不正アクセスがあったとき、これらの機器等１１，１２より不正アクセスがあったことを示す不正アクセス報告１６を集中セキュリティ管理装置１４に非同期で送信するように構成する。また、集中セキュリティ管理装置１４は、機器等１１，１２より非同期で送信される不正アクセス報告１６を受け取り、これら機器等１１，１２を集中管理できるように構成する。本例は以上のように構成し、その他は図４の例と同様に構成する。

【００１１】次に、図２を使用して集中セキュリティ管理装置１４の動作を説明する。まず、ネットワーク構成機器１１、データ処理装置１２の全てに対してセキュリティ情報１５を設定する（ステップ２１）。そして、ネットワーク構成機器１１、データ処理装置１２から非同期で送信される不正アクセス報告１６を受け取る（ステップ２２）。

【００１２】次に、図３を使用して被管理装置であるネットワーク構成機器１１、データ処理装置１２の動作を説明する。まず、ネットワーク構成機器１１、データ処

3

理装置１２は、それぞれ集中セキュリティ管理装置１４からのセキュリティ情報設定要求を受け、自装置にセキュリティ情報１５を設定する（ステップ３１）。そして、ネットワーク構成機器１１、データ処理装置１２は、設定したセキュリティ情報１５に対して、それを犯す不正アクセスを受けると、集中セキュリ管理装置１４に対して不正アクセス報告１６を非同期で送信する（ステップ３２）。

【００１３】実施例２．なお、上記実施例１では、ネットワーク構成機器１１として、多重化装置の場合に付いて説明したが、例えばＰＢＸ、パケット交換装置、ランとランを接続するブリッジやルータ等その他ネットワークを構成するいかなる機器にも適用でき、同様の効果を奏する。また、データ処理装置１２としてコンピュータの場合に付いて説明してが、例えば電話等その他不正アクセスを受け得る計算機室等のドア、電源装置等のその他の機器にも適用でき、同様の効果を奏する。

【００１４】

【発明の効果】以上のように、この発明によれば、被管理装置を構成する複数の機器のセキュリティを集中して管理するセキュリティ管理装置を備え、セキュリティ管理装置は、複数の機器にそれぞれセキュリティ情報を設定すると共に、これら複数の機器より不正アクセスがあったことを示す不正アクセス報告を受け取るようにしたので、セキュリティ管理装置によって複数の機器を集中して管理することができ、複数の機器のセキュリティレベルを同一に保つことができるという効果がある。

4

【００１５】また、被管理装置がネットワークシステムであるときは、ネットワークのどこで不正アクセスが発生しても、即座に発見できるので、ネットワーク全体のセキュリティを高めることができるという効果がある。さらに、１個のセキュリティ管理装置によって被管理装置、例えばネットワークシステムを構成する複数の機器の全てを管理でき、システムを安価に構築できるという効果がある。

【図面の簡単な説明】

【図１】この発明に係るセキュリティ管理システムの一実施例を示す構成図である。

【図２】この発明の一実施例における集中セキュリティ管理装置の動作を説明するための図である。

【図３】この発明の一実施例における被管理の動作を説明するための図である。

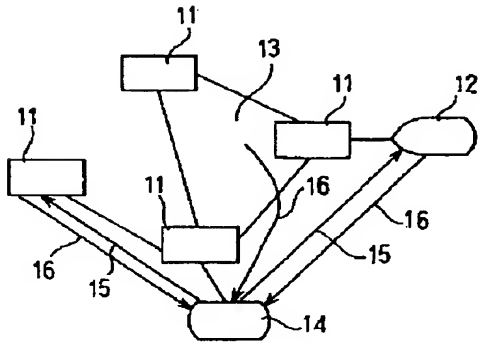
【図４】従来のセキュリティ管理システムを示す構成図である。

【図５】従来のセキュリティ管理システムの動作を説明するための図である。

【符号の説明】

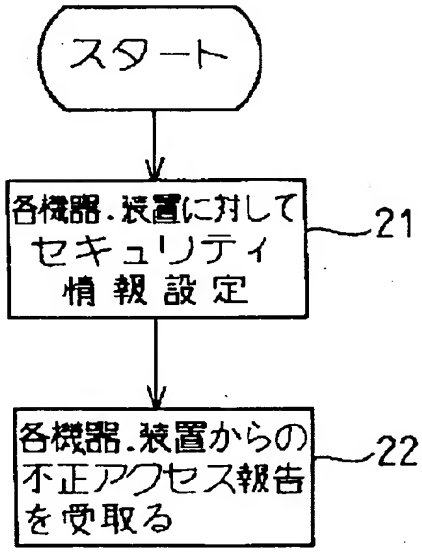
１１　ネットワーク構成機器
１２　データ処理装置
１３　ネットワーク
１４　集中セキュリティ管理装置
１５　セキュリティ情報
１６　被同期イベント

【図１】

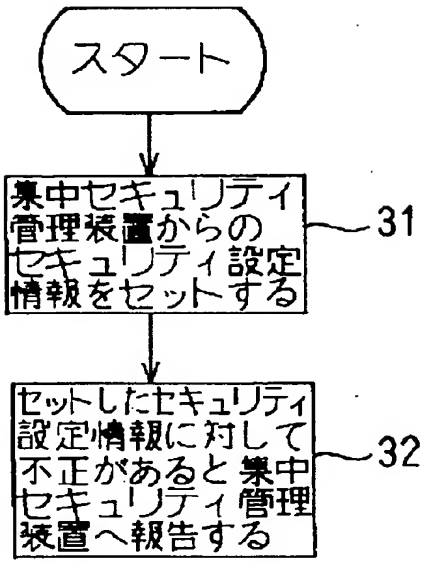


11：ネットワーク構成機器
12：データ処理装置
13：ネットワーク
14：集中セキュリティ管理装置
15：セキュリティ情報
16：不正アクセス報告

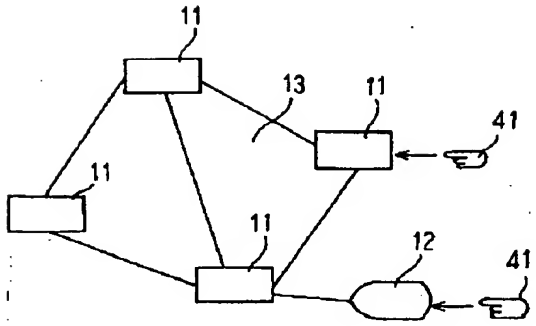
【図２】



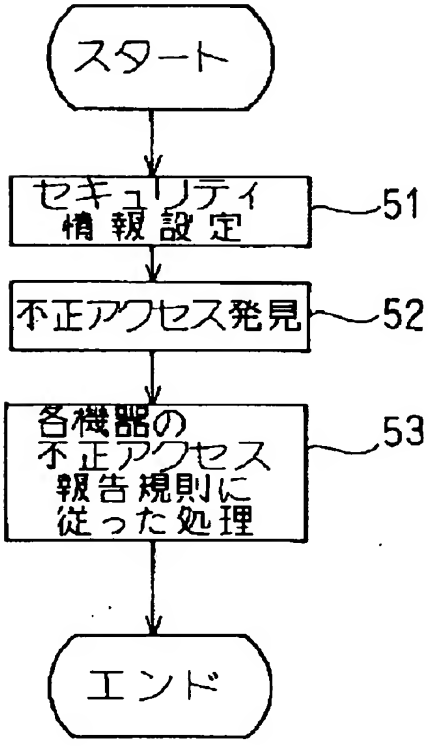
【図３】


スタート
集中セキュリティ管理装置からのセキュリティ設定情報をセットする
31
セットしたセキュリティ設定情報に対して不正があると集中セキュリティ管理装置へ報告する
32

【図４】


11
13
11
41
11
11
12
41

【図５】


スタート
セキュリティ情報設定
51
不正アクセス発見
52
各機器の不正アクセス報告規則に従った処理
53
エンド

【手続補正書】
【提出日】平成４年８月１０日
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】００１３
【補正方法】変更
【補正内容】
【００１３】実施例２．なお、上記実施例１では、ネットワーク構成機器１１として、多重化装置の場合に付いて説明したが、例えばＰＢＸ、パケット交換装置、ＬＡＮ（ＬｏｃａｌＡｒｅａＮｅｔｗｏｒｋ）とＬＡＮを接続するブリッジやルータ等その他ネットワークを構成するいかなる機器にも適用でき、同様の効果を奏する。また、データ処理装置１２としてコンピュータの場合に付いて説明してが、例えば電話等その他不正アクセスを受け得る計算機室等のドア、電源装置等のその他の機器にも適用でき、同様の効果を奏する。

フロントページの続き

(51)Int.Cl.[5]	識別記号	庁内整理番号	Ｆ Ｉ			技術表示箇所
		8529-5K	11/00	310	Z	